Statement of Thomas M. Meiss
Associate General Counsel, Cingular Wireless
Before the Subcommittee on Oversight and Investigations
September 29, 2006

Good morning, Mr. Chairman and distinguished members of the Subcommittee. My name is Tom Meiss and I am Associate General Counsel for Cingular Wireless. Thank you for your invitation to appear today to discuss the important issue of pretexting.

The title of today's hearing includes a question: "Who has Access to Your Call Records?" The only *right* answer to that question, of course, would be "Just you, the customer." Unfortunately, that has not always been the case.

It would be hard to find someone today who has not heard of pretexting for call records. But a year ago, that was far from the case. It is helpful—in fact, it is necessary—to put things in perspective by reviewing the time line of the phenomenon of data brokers and call records from last year to the present. But first I want to point something out. For convenience, we will often today be using the terms "data brokers" and "pretexters". But let's be clear about one thing. They are thieves—data burglars—plain and simple. The term "pretexter" is far too innocuous.

As recently as early 2005, the practice of web-based data brokers pretexting for call records had generated little notice. In spring and early summer of last year, Cingular began to receive some complaints that customers' records had been obtained

through data broker websites. Around the same time, stories were appearing in the press suggesting that pretexting could be a growing problem for businesses. Cingular notified its customer service representatives to be on the lookout for pretexting attempts, and to be especially diligent in verifying callers seeking account information. But by mid-year, we had received only a handful of complaints about the problem—the numbers at the time gave no indication that pretexting by data brokers was a widespread issue.

However, near the end of the summer a series of events changed the picture completely. EPIC, a leading privacy organization, notified the FTC and the FCC that they had identified more than forty websites offering to sell phone records. First a few, then dozens of newspaper and television stories appeared, reporting that it was, indeed, possible to easily obtain cellphone records for a fee.

At the same time, Cingular was conducting investigations to see how this could be happening. We looked for an internal leak of some kind—from an employee, a contractor—what else could explain the apparently absolute certainty with which these websites claimed they could obtain these records? It just did not seem possible that pretexting could be the basis for so many website businesses.

Without yet knowing exactly how the data brokers were getting the call records, we went ahead and made changes to our procedures. We changed our account access policy such that NO call detail records could be provided over the phone to ANYONE--

not even to a verified customer. And we filed lawsuits, first against locatecell.com and then against efindouthetruth.com. We successfully obtained injunctions against the operators of both websites. We have since brought four more lawsuits, against more than 30 different corporate and individual defendants, including five of the data brokers who appeared before this Committee in June.

By the end of January 2006, our litigation was beginning to give us some insight into how the pretexters were operating. We hired an ex-data broker to meet with us in Atlanta. We got a first-hand account of specific ruses that were actually being used by pretexters, and we used that information to create very real examples in a newly revamped training course on pretexting for our reps. A few months ago we engaged an "ethical hacking" firm to test the success of our training by conducting planned pretexting attacks. We will use the results from this testing to continue to refine our employee training and security.

Cingular has *always* been aware of, and focused on, its obligation to protect the privacy of our customers' personal information. To secure sensitive customer information, we employ a wide variety of physical, technological, and procedural safeguards. In each case they are designed to be appropriate for the sensitivity of the information being secured. We have a Privacy Team that monitors new privacy laws and designs appropriate compliance programs. We have organizations devoted to both physical and IT security. We have an interdepartmental committee that focuses on all areas of security across the company. It evaluates current processes and procedures,

and recommends improvements where need is identified. Our Internal Auditors regularly perform targeted audits of various company channels that handle sensitive information.

As we continue to evaluate, refine, and improve our security for customer information, we are mindful not only that we must offer security that is appropriate for the sensitivity of the information, but also that it must be balanced with enabling customers to conveniently access their information, get good customer service, and not be hamstrung with yet another mandatory password that many would rather do without.

We know that this is a fight that will never be over—the data burglars will always be out there, continually evolving their methods, and we will be continually working to counter their efforts. Cingular will *always* be committed to upholding our obligation to protect the privacy of our customers' personal information.